



**Making Life Easier**  
**888-874-7290**



## Protecting Yourself From Identity Theft

---

REVIEWED DEC 26, 2006

You probably wouldn't think of leaving your car, purse or wallet wide open, unwatched and unprotected from theft. But you may not be so careful about your personal information such as your phone number, address, Social Security number, driver's license number and credit card numbers. These are valuable property, too. If they fall into the hands of identity thieves, you could lose not only a lot of money but also your good name.

### **New technologies make it easier**

Identity theft is not a new form of crime, but it's especially well-suited to the new world of automated financial transactions. Technologies such as the Internet enable people to buy goods on credit without even a telephone call, much less a face-to-face encounter. So it's easier than ever to fake an identity by getting crucial personal data.

Add to that the potential of online encounters to extract private information, and you have plenty of new opportunities for ID larceny. "The Internet makes [identity theft] easier," says Paul Fichtman, head of the Philadelphia risk-management firm InternetClearinghouse, "So as a result, the criminals take the path of least resistance."

### **Junk mail can give you away**

Meanwhile, crooks continue to steal identities in more old-fashioned ways such as "Dumpster diving," in which they prowl through trash to find mail or other pieces of paper with personal data. You may think you've ripped or shredded everything that could identify you, but don't be so sure. All those unsolicited credit card offers, which many people throw away unopened, can have critical data on them.

The telephone and e-mail are also potent tools for so-called "pretexters," who can skillfully put you off your guard. Fichtman says someone posing as a bank representative might tell you, via a phone call or an unsolicited e-mail, that he's checking out suspicious activity on a credit card and wants to know if it's yours, so he'll ask for your credit card numbers.

### **From fake addresses to auto loans**

Once a thief gets your numbers, he can start posing as you and, of course, stealing from you. Diane Terry, who heads the Fraud Victim Assistance Department for the credit reporting firm TransUnion, says a thief may call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. “The fraudster then runs up charges on your account,” says Terry. “Because your bills are being sent to the new address, it may take some time before you realize there’s a problem.”

Identity thieves can do damage in several other ways, Terry says. They can:

- open a new credit card account with your name, date of birth and Social Security number
- set up phone or wireless service in your name
- open a bank account in your name and write bad checks on it
- file for bankruptcy under your name
- counterfeit checks or debit cards to drain your bank account
- buy cars by taking out auto loans in your name

## Protecting yourself

In short, identity thieves can clean you out, ruin your credit and may even get you falsely accused of a crime. Manhattan lawyer Scott Lavin, who has represented victims trying to get their good names back, calls identity theft “a kind of economic terrorism.”

How can you protect yourself from it? Experts suggest steps such as these:

- **Unless you have initiated the call, or have made an initial inquiry via e-mail, don’t give out personal data** such as your address, phone number and driver’s license number, credit card or Social Security number, to anyone. Your Social Security number is especially sensitive. Give it out only when absolutely necessary, and use other identifiers if possible.
- **Cut, tear or shred anything with personal data on it before throwing it in the trash.** This includes offers you get for financial services such as credit cards.
- **Avoid carrying your Social Security card, birth certificate or passport.** Keep them in a secure place. Reduce personal data in your wallet to a minimum—no account numbers or PINs. Carry only the credit or ATM cards you regularly use.
- **Don’t have your Social Security or driver’s license number printed on your checks.** If asked for your Social Security number when you pay by check, Lavin says it’s “perfectly legal” to refuse.
- **Maintain careful records** of your banking and financial records.
- **Be aware of people who might try to eavesdrop** on information that you give out orally.
- **Be suspicious of telephone solicitors or spam-email** requesting personal information for unbelievable offers, including lottery or sweepstakes ploys.
- **Guard personal account passwords.** Don’t use your mother’s maiden name, your birth date or the last four digits of your social security number for passwords.
- **Verify all Web sites for authenticity before you make a purchase online using a credit card.** Many Web sites now register their authenticity with third parties such as VeriSign.com or Truste.org for this purpose.
- **Learn to pick up signs of trouble.** Get familiar with the billing cycle for your credit

cards, so that you can notice if they've stopped arriving (an identity thief could have changed the mailing address). Order a credit report at least once a year to ensure accuracy (see the numbers for rating agencies under "Resources" below).

### **Take action in case of theft**

Act quickly if you see evidence of theft such as inaccuracies on your credit report, unfamiliar charges on your credit card or bills for purchases you didn't make. The Federal Trade Commission says you should take these three steps immediately:

- Call the fraud-reporting numbers at the three credit-rating services: Experian, TransUnion and Equifax (see "Resources," below).
- For any accounts that have been fraudulently accessed or opened, call the security departments of the creditors or financial institutions. Close the accounts. Put passwords—not your mother's maiden name—on any new accounts you open.
- Report any identity theft to your local police, or to the police in the area where the theft occurred. Get a copy of the police report in case a bank, credit card company or others later need to verify the crime.

Terry also advises alerting all creditors listed on your credit report—stores, credit-card companies and other grantors of credit—to the fraud. Call the credit grantors directly to have inaccurate information removed. She also says you should ask credit reporting agencies to flag your name and Social Security number so that you'll be notified if anyone tries to obtain personal credit using your personal information. And if a bank is involved, she says, call the FBI as well as the local police.

### **Resources**

To report identity theft to credit-rating agencies call, Equifax at (888) 766-0008, Experian at (888) EXPERIAN (888-397-3742) and TransUnion at (800) 680-7289.

To order credit reports, call Equifax at (800) 997-2493, Experian at (888) EXPERIAN and TransUnion at (800) 888-4213.

Whether you have a problem or you just want to educate yourself, the best place to visit is the Federal Trade Commission's Web site devoted to identity theft. Go to [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). You'll find a wealth of guides and links covering the problem and explaining what to do both to prevent identity theft and to clear your name. Note the FTC's "ID Theft Affidavit," which you can use to alert a long list of creditors, associations and rating firms if you've been a victim of identity theft.

**By Tom Gray**

© 2001 Achieve Solutions

**Making Life Easier:** 888-874-7290

<https://www.achievementsolutions.net/achievementsolutions/en/kcmle/>